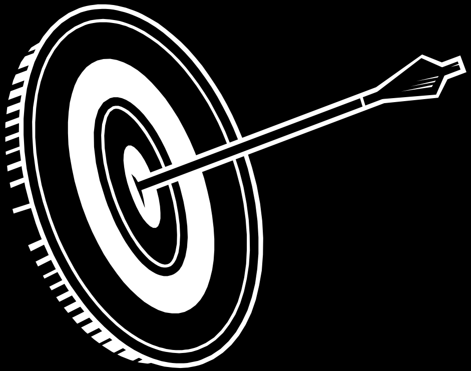
Recent Targeting Phishing Attacks

Jay Krous
Computer Protection Program
www.lbl.gov/cyber

LBNL CFO is being targeted

- Two attacks (June 8, Nov 12)
- Malicious email to control your computer
- Why CFO? Likely due to financial data
- Who is doing this?
- 6 recipients in each attack
  - One successful compromise
  - One partially successful



Who was targeted?

- AKChan, CKLou, HCheng, JWLee, KCHeung, KWinters, MAStrickland, MTHach, NMLee, PMMeo, RSayson, VBEllis
- If you're not on this list, your likely next!
- I want to help you avoid these attacks

A successful compromise of LBNL financial data would be very bad

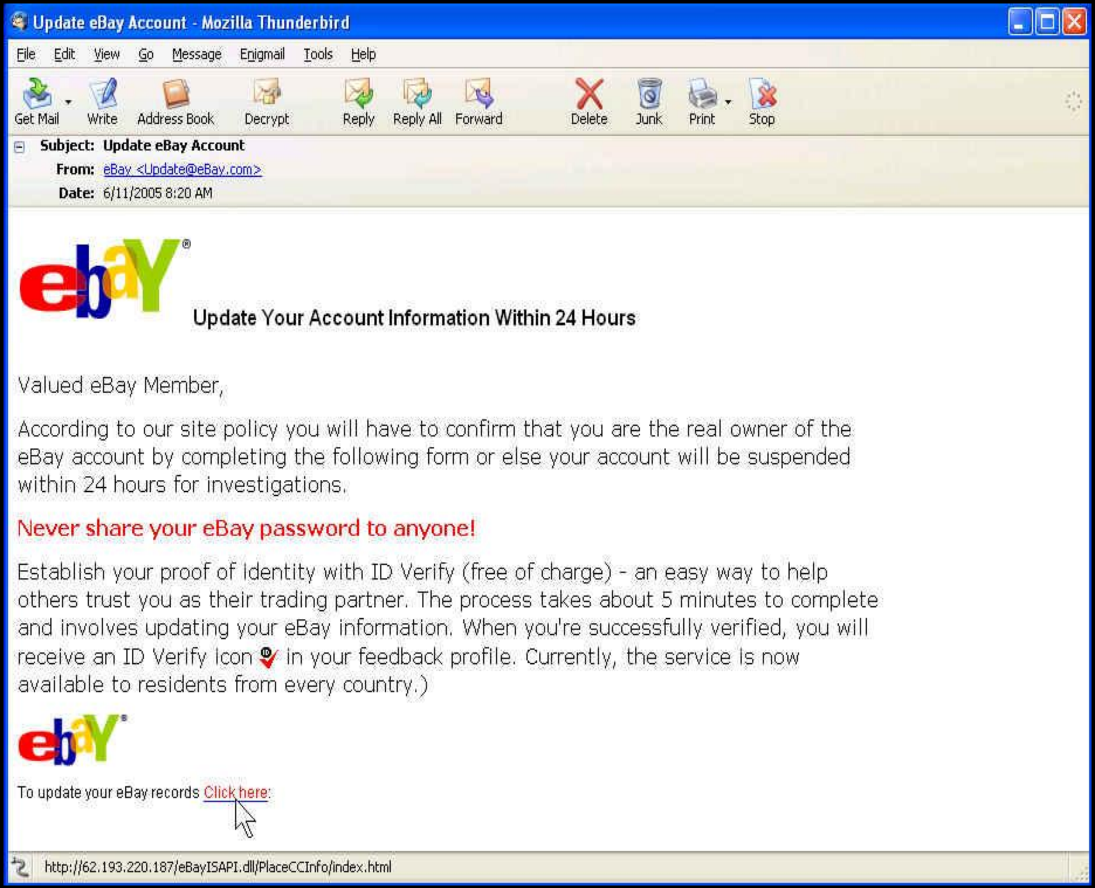
- LBNL would be required by law to report it
- Would likely make national media
- It could put our contract at risk
- PPNL and ORNL unplugged the network for a day
- You don’t want to be “that person”

What is phishing?

- You – the fish
- Email – the bait
- Bad guy – the fisherman
- Financial gain – the catch

Key Components

- Forged emails
  - From address is easily spoofed
  - Graphics easily duplicated
- Attachments and links
- Control you computer
- Driven by financial gain


Update eBay Account - Mozilla Thunderbird
File Edit View Go Message Enigmail Tools Help
Get Mail
Write
Address Book
Decrypt
Reply
Reply All
Forward
Delete
Junk
Print
Stop

Subject: Update eBay Account

From: eBay <Update@eBay.com>

Date: 6/11/2005 8:20 AM

Update Your Account Information Within 24 Hours

Valued eBay Member,

According to our site policy you will have to confirm that you are the real owner of the eBay account by completing the following form or else your account will be suspended within 24 hours for investigations.

Never share your eBay password to anyone!

Establish your proof of identity with ID Verify (free of charge) - an easy way to help others trust you as their trading partner. The process takes about 5 minutes to complete and involves updating your eBay information. When you're successfully verified, you will receive an ID Verify icon ✓ in your feedback profile. Currently, the service is now available to residents from every country.)

To update your eBay records Click here:

http://62.193.220.187/eBayISAPI.dll/PlaceCCInfo/index.html

Most of us recognize phishing

I HAVE A NEW HOBBY. IT'S CALLED PHISHING.
scottadams@aol.com
www.dilbert.com
I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFORMATION AND USE IT TO STEAL THE MONEY THEY DON'T DESERVE.
© 2005 Scott Adams, Inc./Dist. by UFS, Inc.
8-12-05
Dear Customer,
This is your bank. We forgot your social security number and password. Why don't you send them to us so we can protect your money.
Sincerely,
I. B. Banker
LOOKS LEGIT.

© Scott Adams, Inc./Dist. by UFS, Inc.

Targeted phishing is harder

- Forged emails
- Attachments and links
- Control your computer
- Driven by financial gain

- Specific to you or your work
- Refers to people/places/things you know
- Carefully written to fool you
- May appear innocuous

Subject: AIAA ASM Meeting in Reno

Dear Solid Rockets Technical Committee Members,

Attached is the agenda for our upcoming meeting in Reno. Please let me know whether or not you will be attending so that we can get a proper head-count for the dinner on Tuesday.

Attached: agenda.exe

Subject: HSPD-12 Identification Briefing

Body: As identified by Executive and Department of Energy (DOE) orders, all DOE and National Nuclear Security Administration (NNSA) Federal and contractor employees will be participating in the switch to the new HSPD-12 badge system. The DOE HSPD-12 Identification Briefing (HIB).... ...EMPLOYEES RECEIVING THIS NOTICE ARE REQUIRED TO PRINT THIS BRIEFING IMMEDIATELY.

Link: http://www.energyoclc.net/HSPD12Training/

Subject: Please send the account number

Attached is the file to use.

Attached: project.mdb

Subject: www.vertecal.com registration

Thank you for registering with vertical. Your temporary PIN is: 459578. Once you enter this PIN, you'll be prompted to change it to a different 6-digit code of your choosing. If you encounter any difficulty with the site registration process, please call us 24 hours a day, 7 days a week.

Link: http://www.vertecal.com/support-documentation.html

From: Centers for Disease Control <programs@cdc.govname>
Subject: Government Health Program

In attention of [Real LBNL Manager] at Lawrence Berkeley Lab. Within the last few years there has been a continue increasing of work-related diseases....

Centers for Disease Control an Prevention (CDC) has started a graduate program to study this issue. This is a Governmental Program and your duty is to verify that the attachment you`ve received is complete (if not you can find it here), and forward it to all.

Link: http://www.so-me.net/class/DiseasePrevention.doc

Target phishing is an increasing threat

- It works!
- Other vectors are increasingly difficult
- Hard to battle technically
- Dependant upon user awareness

Tips

- Recognize common attack themes
  - Vague message
  - Click for more information
  - Official looking
- Have you every heard of this before?
- Think twice - every time
- Not sure, send to cppm@lbl.gov
- Don’t trash it, send to cppm@lbl.gov

Resources to help you

- http://www.lbl.gov/cyber
  - Computer Security Annual Refresher
  - Updated list of targeted phishing examples
  - Cyber Social Engineering Training

- Mail cppm@lbl.gov